FIG. 1

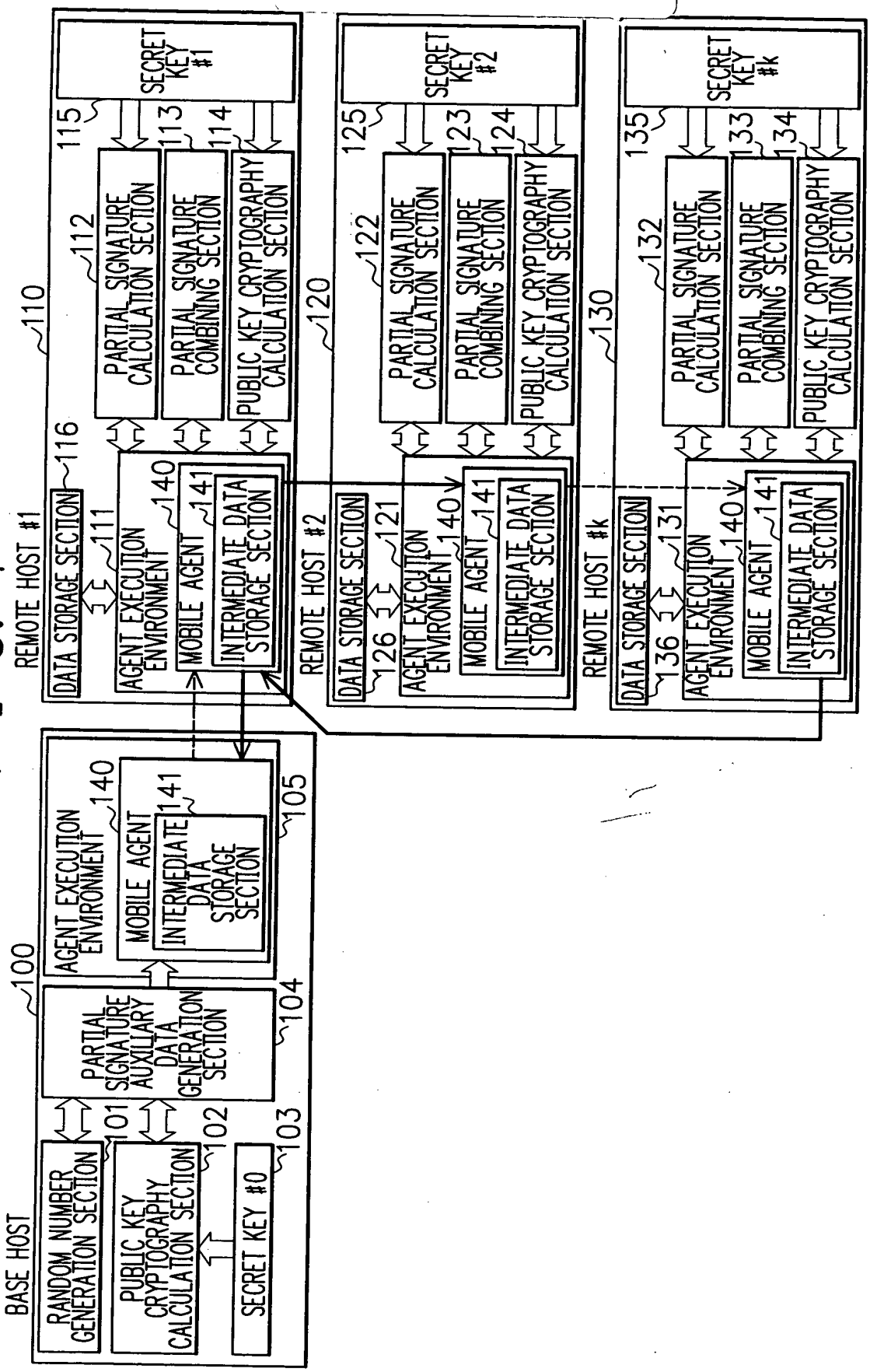

BASE HOST
100
RANDOM NUMBER GENERATION SECTION
101
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
102
SECRET KEY #0
103
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
104
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
105
REMOTE HOST #1
110
DATA STORAGE SECTION
116
AGENT EXECUTION ENVIRONMENT
111
MOBILE AGENT
140
141
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
112
PARTIAL SIGNATURE COMBINING SECTION
113
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
114
SECRET KEY #1
115
REMOTE HOST #2
120
DATA STORAGE SECTION
121
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
126
PARTIAL SIGNATURE CALCULATION SECTION
122
PARTIAL SIGNATURE COMBINING SECTION
123
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
124
SECRET KEY #2
125
REMOTE HOST #k
130
DATA STORAGE SECTION
131
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
136
PARTIAL SIGNATURE CALCULATION SECTION
132
PARTIAL SIGNATURE COMBINING SECTION
133
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
134
SECRET KEY #k
135

FIG. 2

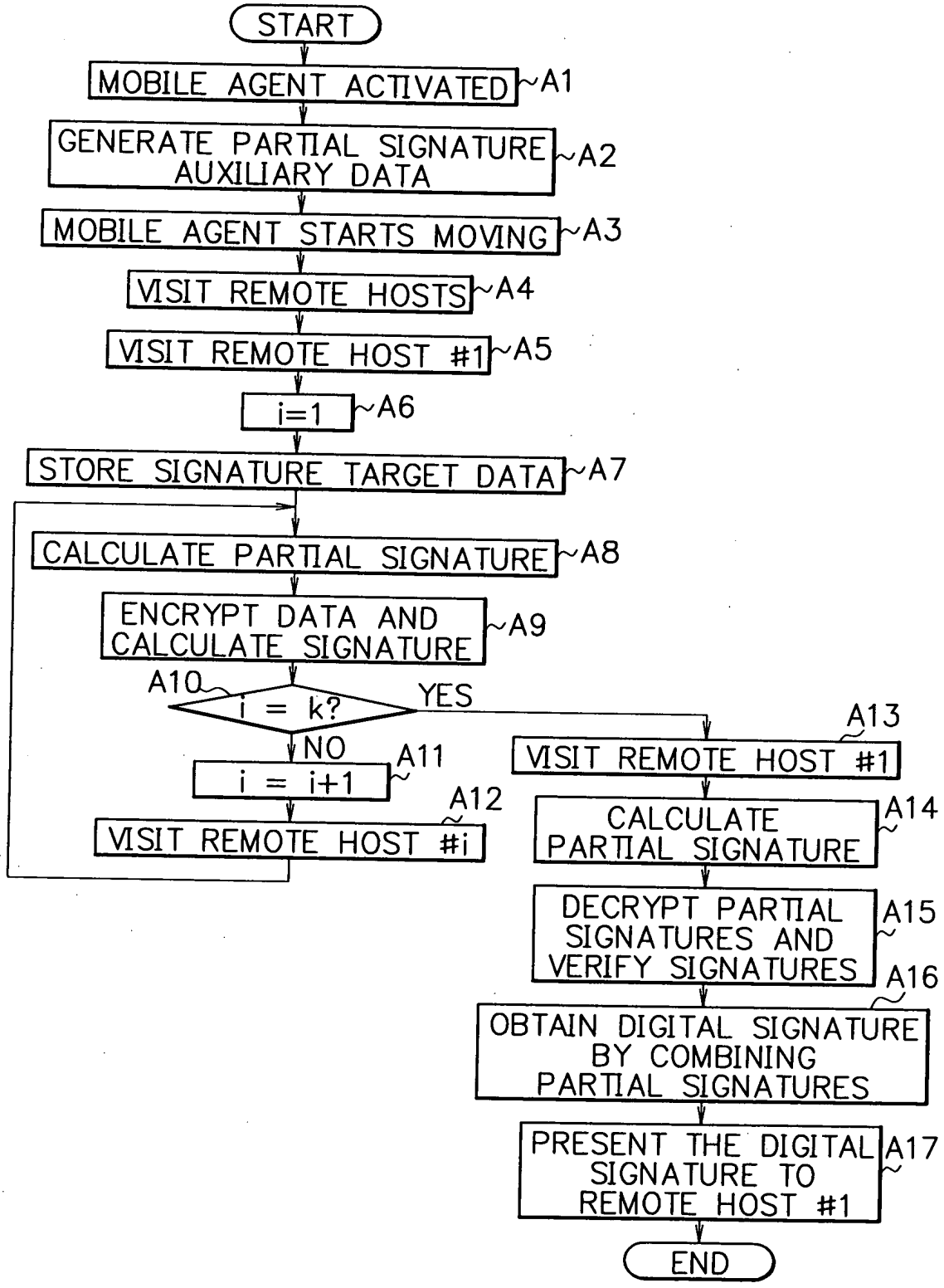

START
MOBILE AGENT ACTIVATED
A1
GENERATE PARTIAL SIGNATURE AUXILIARY DATA
A2
MOBILE AGENT STARTS MOVING
A3
VISIT REMOTE HOSTS
A4
VISIT REMOTE HOST #1
A5
i=1
A6
STORE SIGNATURE TARGET DATA
A7
CALCULATE PARTIAL SIGNATURE
A8
ENCRYPT DATA AND CALCULATE SIGNATURE
A9
A10
i = k?
YES
NO
A11
i = i+1
A12
VISIT REMOTE HOST #i
A13
VISIT REMOTE HOST #1
A14
CALCULATE PARTIAL SIGNATURE
A15
DECRYPT PARTIAL SIGNATURES AND VERIFY SIGNATURES
A16
OBTAIN DIGITAL SIGNATURE BY COMBINING PARTIAL SIGNATURES
A17
PRESENT THE DIGITAL SIGNATURE TO REMOTE HOST #1
END

FIG. 3

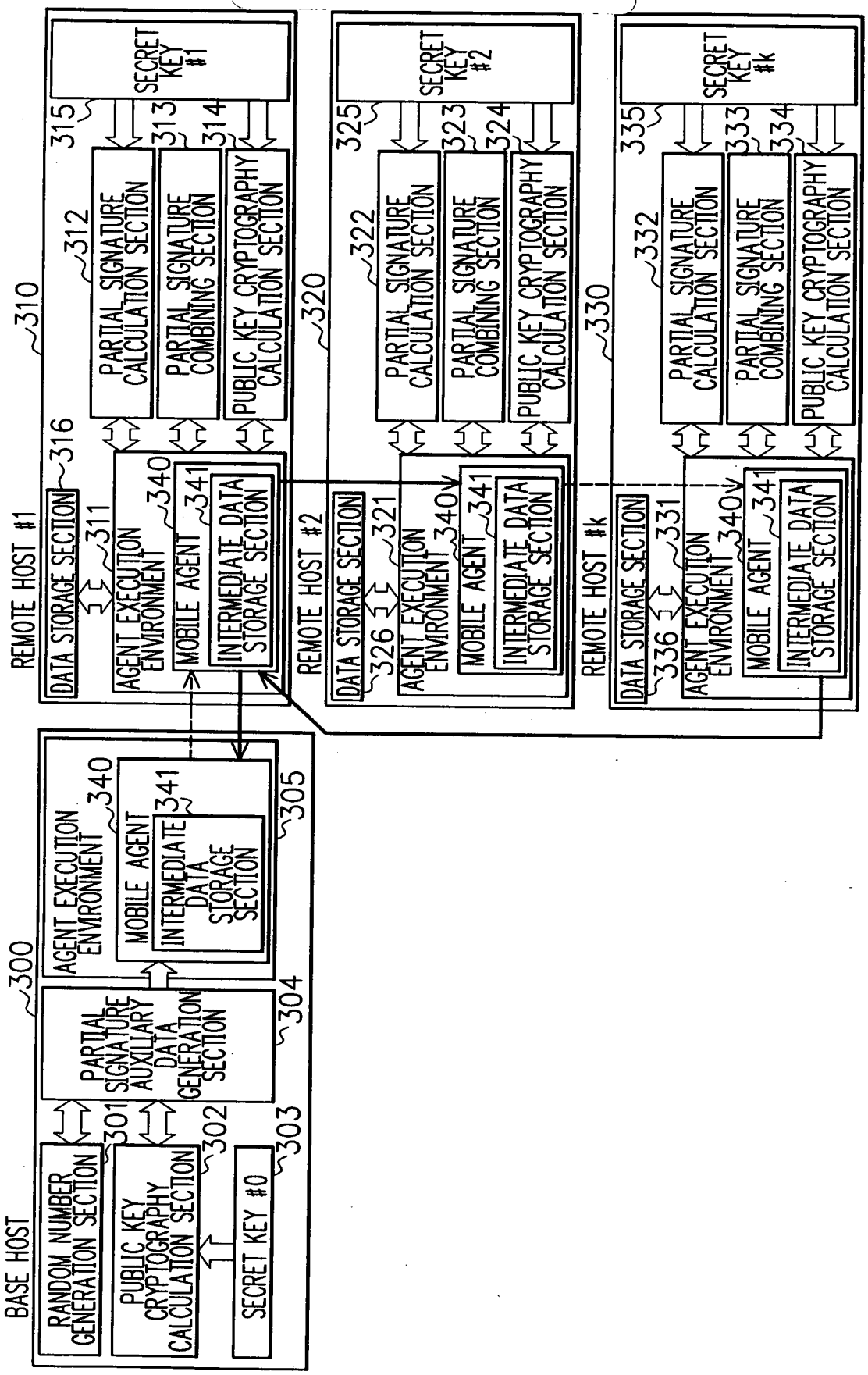

BASE HOST
300
RANDOM NUMBER GENERATION SECTION
301
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
302
SECRET KEY #0
303
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
304
AGENT EXECUTION ENVIRONMENT
340
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
305
REMOTE HOST #1
310
DATA STORAGE SECTION
316
AGENT EXECUTION ENVIRONMENT
311
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
340
PARTIAL SIGNATURE CALCULATION SECTION
312
PARTIAL SIGNATURE COMBINING SECTION
313
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
314
SECRET KEY #1
315
REMOTE HOST #2
320
DATA STORAGE SECTION
326
AGENT EXECUTION ENVIRONMENT
321
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
340
PARTIAL SIGNATURE CALCULATION SECTION
322
PARTIAL SIGNATURE COMBINING SECTION
323
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
324
SECRET KEY #2
325
REMOTE HOST #k
330
DATA STORAGE SECTION
336
AGENT EXECUTION ENVIRONMENT
331
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
340
PARTIAL SIGNATURE CALCULATION SECTION
332
PARTIAL SIGNATURE COMBINING SECTION
333
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
334
SECRET KEY #k
335

FIG. 4

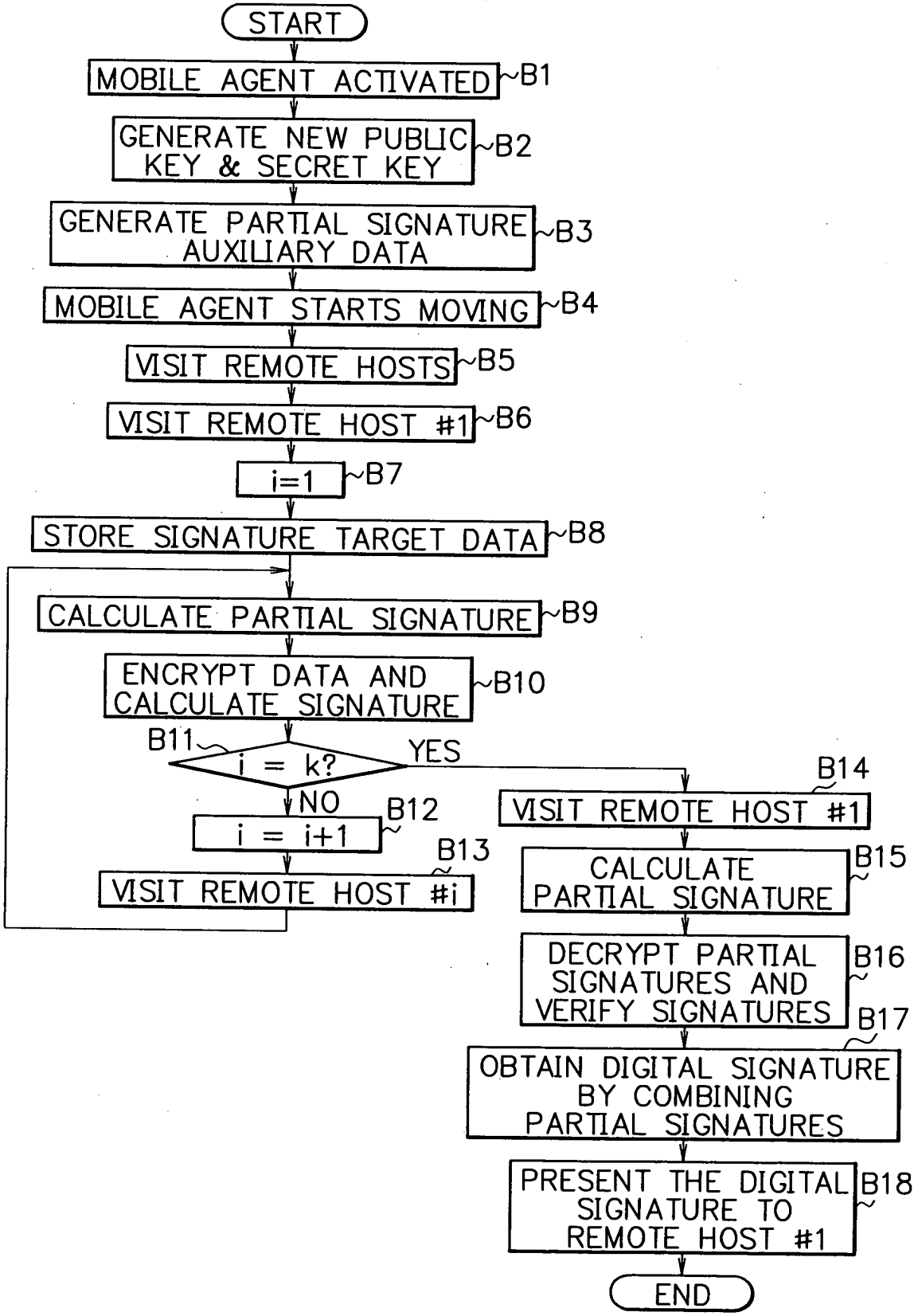

START
MOBILE AGENT ACTIVATED
B1
GENERATE NEW PUBLIC KEY & SECRET KEY
B2
GENERATE PARTIAL SIGNATURE AUXILIARY DATA
B3
MOBILE AGENT STARTS MOVING
B4
VISIT REMOTE HOSTS
B5
VISIT REMOTE HOST #1
B6
i=1
B7
STORE SIGNATURE TARGET DATA
B8
CALCULATE PARTIAL SIGNATURE
B9
ENCRYPT DATA AND CALCULATE SIGNATURE
B10
B11
i = k?
YES
NO
B12
i = i+1
B13
VISIT REMOTE HOST #i
B14
VISIT REMOTE HOST #1
B15
CALCULATE PARTIAL SIGNATURE
B16
DECRYPT PARTIAL SIGNATURES AND VERIFY SIGNATURES
B17
OBTAIN DIGITAL SIGNATURE BY COMBINING PARTIAL SIGNATURES
B18
PRESENT THE DIGITAL SIGNATURE TO REMOTE HOST #1
END

FIG. 5

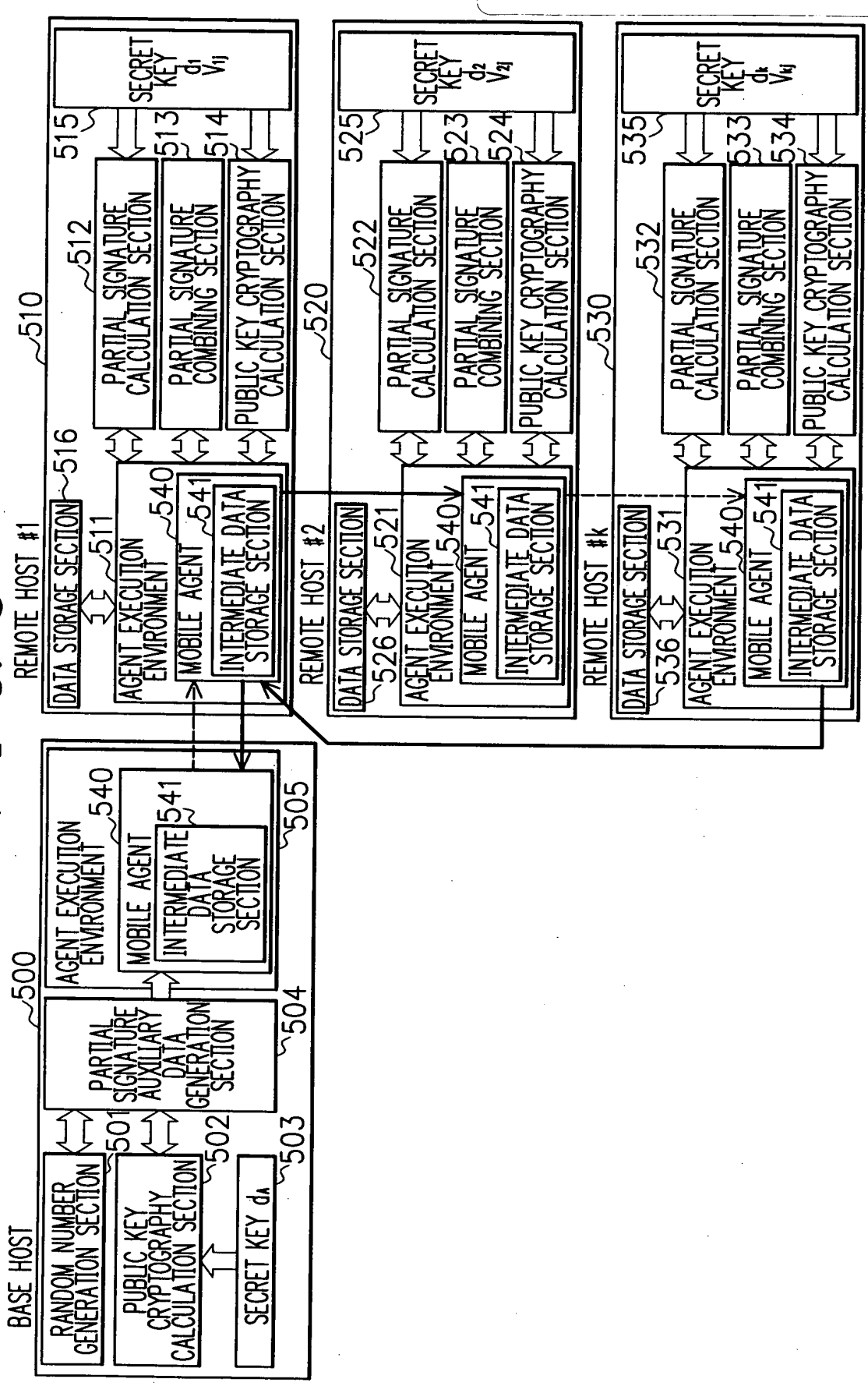

BASE HOST
500
RANDOM NUMBER GENERATION SECTION
501
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
502
SECRET KEY d_A
503
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
504
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
505
REMOTE HOST #1
510
DATA STORAGE SECTION
516
511
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
512
PARTIAL SIGNATURE COMBINING SECTION
513
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
514
SECRET KEY d_1 V_{1j}
515
REMOTE HOST #2
520
DATA STORAGE SECTION
526
521
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
522
PARTIAL SIGNATURE COMBINING SECTION
523
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
524
SECRET KEY d_2 V_{2j}
525
REMOTE HOST #k
530
DATA STORAGE SECTION
536
531
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
532
PARTIAL SIGNATURE COMBINING SECTION
533
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
534
SECRET KEY d_k V_{kj}
535

FIG. 6

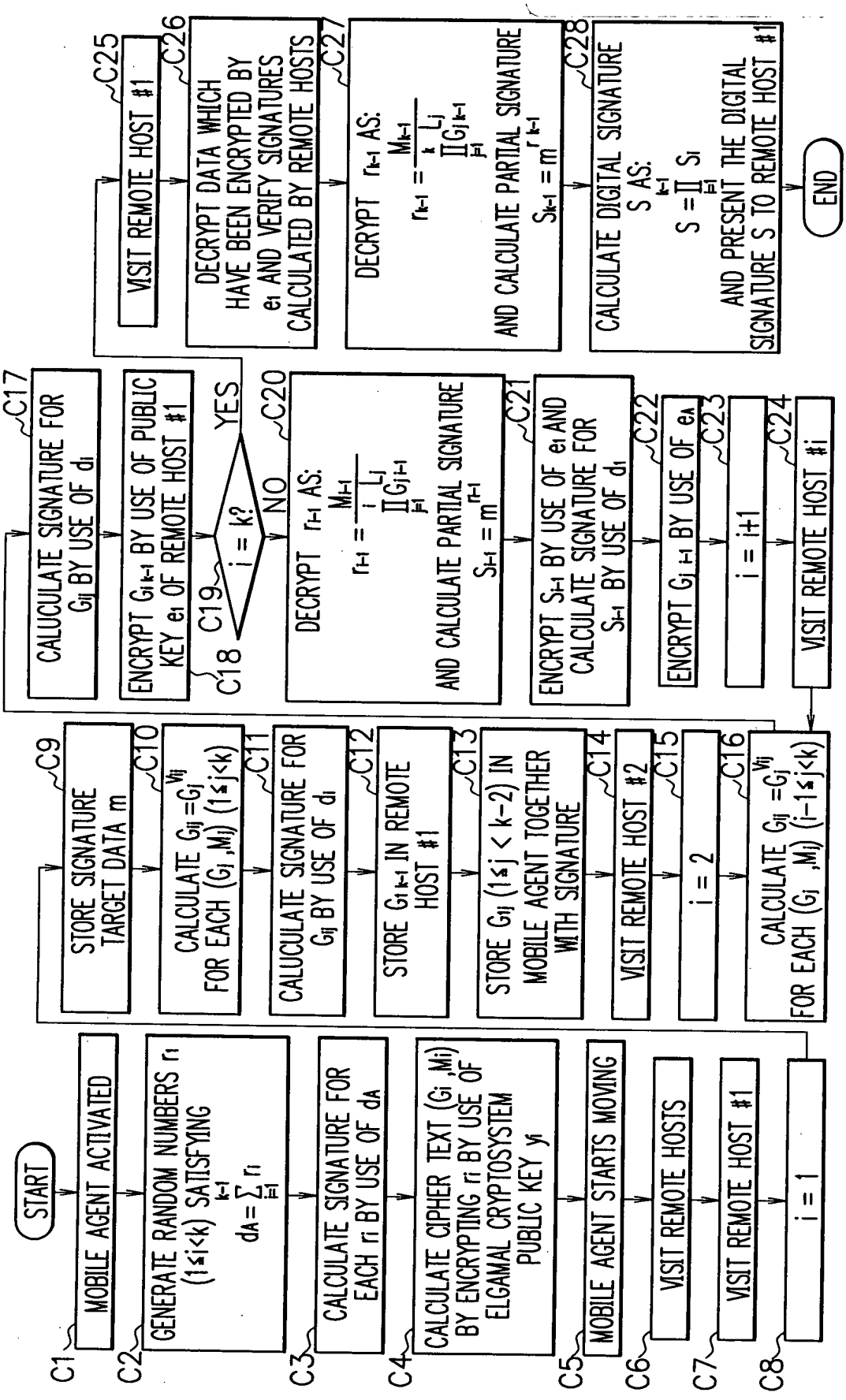

START
C1 MOBILE AGENT ACTIVATED
C2 GENERATE RANDOM NUMBERS r_i ($1 \le i < k$) SATISFYING $d_A = \sum_{i=1}^{k-1} r_i$
C3 CALCULATE SIGNATURE FOR EACH r_i BY USE OF d_A
C4 CALCULATE CIPHER TEXT (G_i, M_i) BY ENCRYPTING r_i BY USE OF ELGAMAL CRYPTOSYSTEM PUBLIC KEY y_i
C5 MOBILE AGENT STARTS MOVING
C6 VISIT REMOTE HOSTS
C7 VISIT REMOTE HOST #1
C8 i = 1
C9 STORE SIGNATURE TARGET DATA m
C10 CALCULATE $G_{ij} = G_j^{V_{ij}}$ FOR EACH (G_j, M_j) ($1 \le j < k$)
C11 CALCULATE SIGNATURE FOR G_{ij} BY USE OF d_i
C12 STORE $G_{i\,k-1}$ IN REMOTE HOST #1
C13 STORE G_{ij} ($1 \le j < k-2$) IN MOBILE AGENT TOGETHER WITH SIGNATURE
C14 VISIT REMOTE HOST #2
C15 i = 2
C16 CALCULATE $G_{ij} = G_j^{V_{ij}}$ FOR EACH (G_j, M_j) ($i-1 \le j < k$)
C17 CALCULATE SIGNATURE FOR G_{ij} BY USE OF d_i
C18 ENCRYPT $G_{i\,k-1}$ BY USE OF PUBLIC KEY e_1 OF REMOTE HOST #1
C19 i = k?
YES
NO
C20 DECRYPT r_{i-1} AS: $r_{i-1} = \frac{M_{i-1}}{\prod_{j=1}^{i} L_j G_{j\,i-1}}$ AND CALCULATE PARTIAL SIGNATURE $S_{i-1} = m^{r_{i-1}}$
C21 ENCRYPT S_{i-1} BY USE OF e_1 AND CALCULATE SIGNATURE FOR S_{i-1} BY USE OF d_i
C22 ENCRYPT $G_{j\,i-1}$ BY USE OF e_A
C23 i = i+1
C24 VISIT REMOTE HOST #i
C25 VISIT REMOTE HOST #1
C26 DECRYPT DATA WHICH HAVE BEEN ENCRYPTED BY e_1 AND VERIFY SIGNATURES CALCULATED BY REMOTE HOSTS
C27 DECRYPT r_{k-1} AS: $r_{k-1} = \frac{M_{k-1}}{\prod_{j=1}^{k} L_j G_{j\,k-1}}$ AND CALCULATE PARTIAL SIGNATURE $S_{k-1} = m^{r_{k-1}}$
C28 CALCULATE DIGITAL SIGNATURE S AS: $S = \prod_{i=1}^{k-1} S_i$ AND PRESENT THE DIGITAL SIGNATURE S TO REMOTE HOST #1
END

FIG. 7

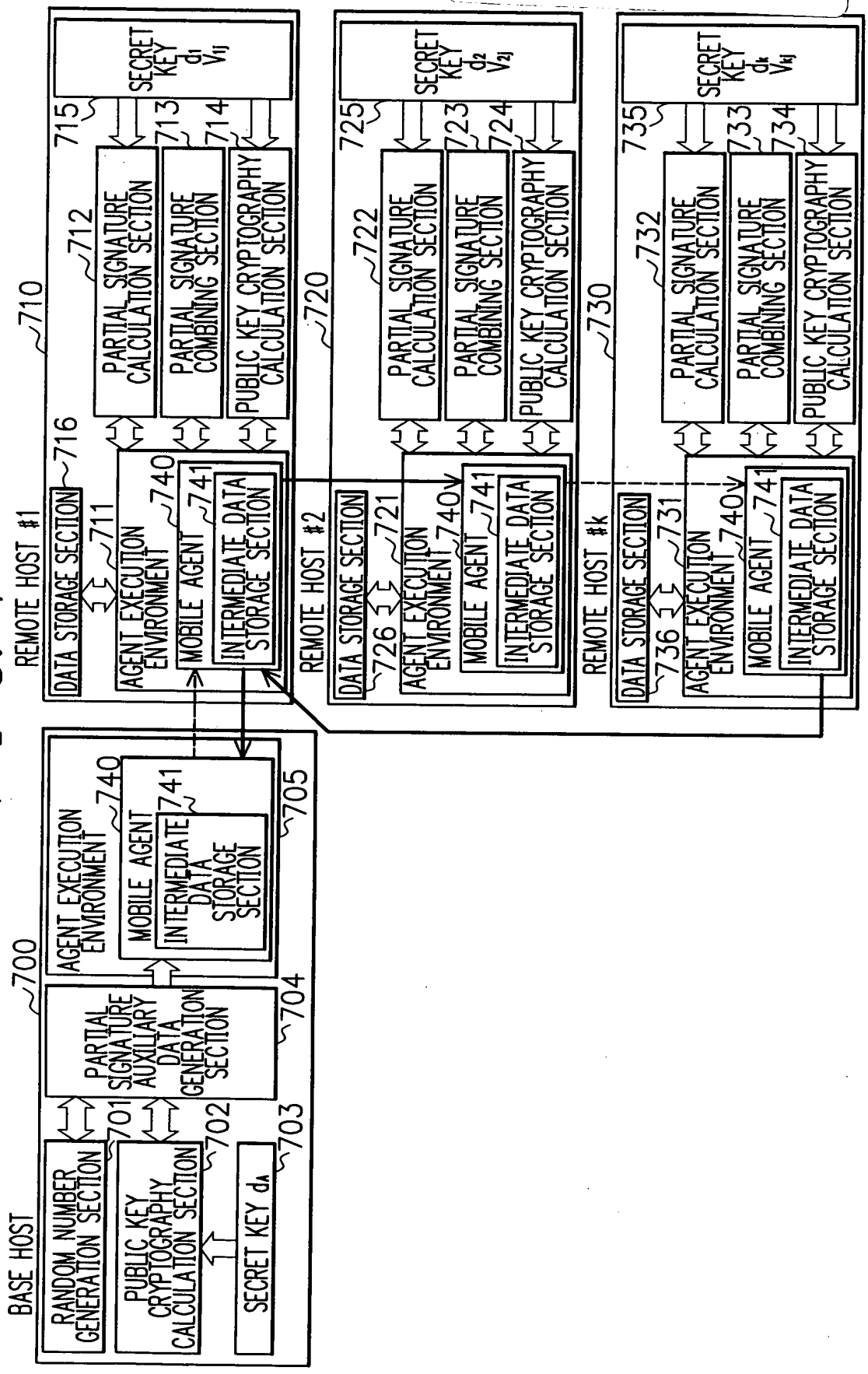
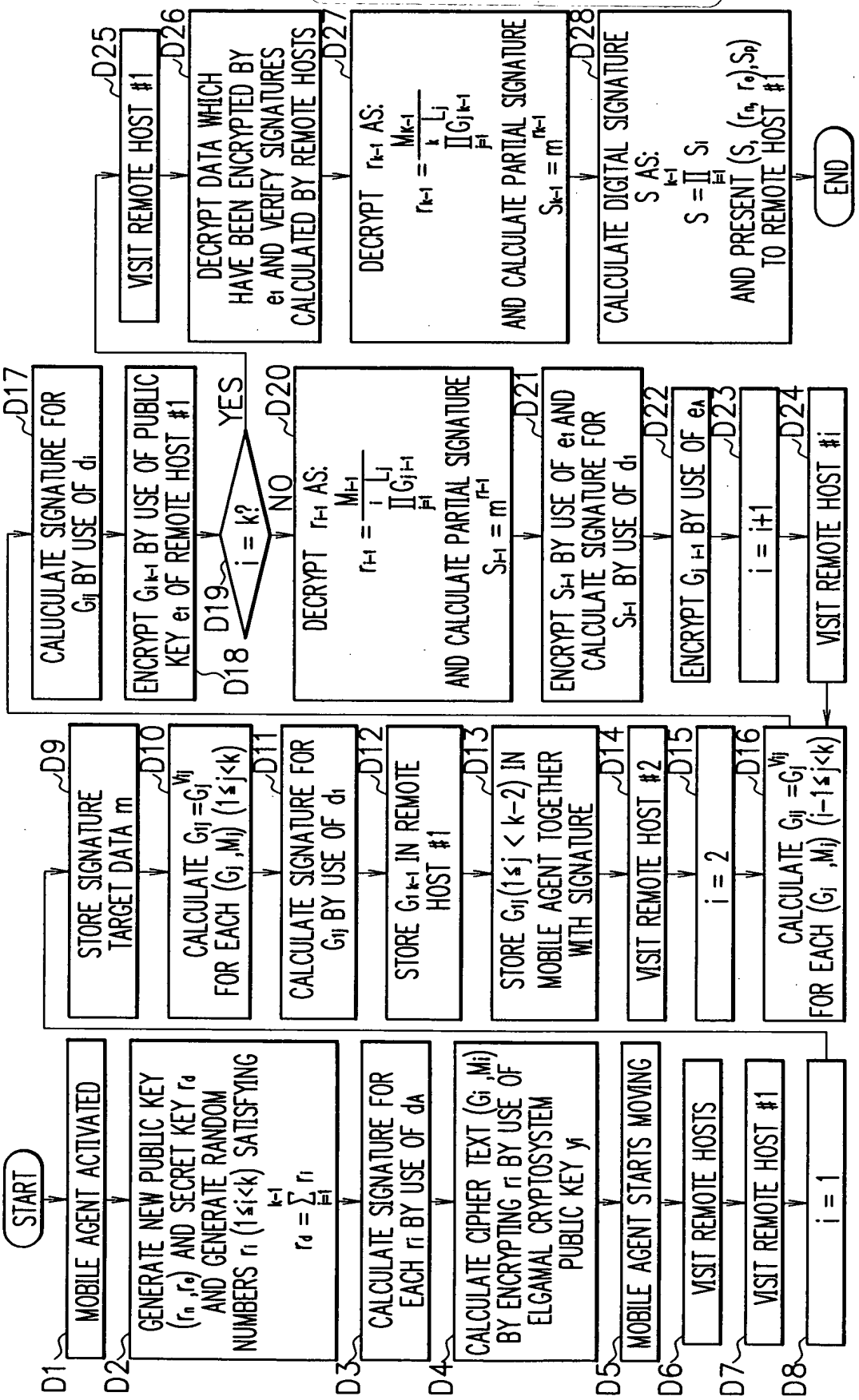

BASE HOST
700
RANDOM NUMBER GENERATION SECTION
701
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
702
SECRET KEY d_A
703
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
704
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
705
REMOTE HOST #1
710
DATA STORAGE SECTION
716
711
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
712
PARTIAL SIGNATURE COMBINING SECTION
713
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
714
SECRET KEY d_1 V_{1j}
715
REMOTE HOST #2
720
DATA STORAGE SECTION
726
721
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
722
PARTIAL SIGNATURE COMBINING SECTION
723
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
724
SECRET KEY d_2 V_{2j}
725
REMOTE HOST #k
730
DATA STORAGE SECTION
736
731
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
732
PARTIAL SIGNATURE COMBINING SECTION
733
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
734
SECRET KEY d_k V_{kj}
735

FIG. 8


START
D1 MOBILE AGENT ACTIVATED
D2 GENERATE NEW PUBLIC KEY (rn, rd) AND SECRET KEY rd AND GENERATE RANDOM NUMBERS ri (1≤i<k) SATISFYING rd = Σ ri (i=1 to k-1)
D3 CALCULATE SIGNATURE FOR EACH ri BY USE OF dA
D4 CALCULATE CIPHER TEXT (Gi, Mi) BY ENCRYPTING ri BY USE OF ELGAMAL CRYPTOSYSTEM PUBLIC KEY yi
D5 MOBILE AGENT STARTS MOVING
D6 VISIT REMOTE HOSTS
D7 VISIT REMOTE HOST #1
D8 i = 1
D9 STORE SIGNATURE TARGET DATA m
D10 CALCULATE Gij = Gj^Vij FOR EACH (Gj, Mj) (1≤j<k)
D11 CALCULATE SIGNATURE FOR Gij BY USE OF di
D12 STORE Gi k-1 IN REMOTE HOST #1
D13 STORE Gij(1≤j < k-2) IN MOBILE AGENT TOGETHER WITH SIGNATURE
D14 VISIT REMOTE HOST #2
D15 i = 2
D16 CALCULATE Gij = Gj^Vij FOR EACH (Gj, Mj) (i-1≤j<k)
D17 CALUCULATE SIGNATURE FOR Gij BY USE OF di
D18 ENCRYPT Gi k-1 BY USE OF PUBLIC KEY e1 OF REMOTE HOST #1
D19 i = k?
YES
NO
D20 DECRYPT ri-1 AS: ri-1 = Mi-1 / (Π Gj i-1 ^ Lj) (j=1 to i-1) AND CALCULATE PARTIAL SIGNATURE Si-1 = m^ri-1
D21 ENCRYPT Si-1 BY USE OF e1 AND CALCULATE SIGNATURE FOR Si-1 BY USE OF di
D22 ENCRYPT Gj i-1 BY USE OF eA
D23 i = i+1
D24 VISIT REMOTE HOST #i
D25 VISIT REMOTE HOST #1
D26 DECRYPT DATA WHICH HAVE BEEN ENCRYPTED BY e1 AND VERIFY SIGNATURES CALCULATED BY REMOTE HOSTS
D27 DECRYPT rk-1 AS: rk-1 = Mk-1 / (Π Gj k-1 ^ Lj) (j=1 to k) AND CALCULATE PARTIAL SIGNATURE Sk-1 = m^rk-1
D28 CALCULATE DIGITAL SIGNATURE S AS: S = Π Si (i=1 to k-1) AND PRESENT (S, (rn, rd), S0) TO REMOTE HOST #1
END